Глава 3 – Многочлены над полем

Билет 1: *Сложение и умножение многочленов. Степень многочлена. Свойства.*

Определение

Пусть K — коммутативное кольцо.

Коммутативное кольцо - кольцо с коммутативностью умножения (ассоциативность +*, коммутативность +*, 0, обратный элемент по +, дистрибутивность)

1) *Кольцо многочленов* над K состоит из бесконечных последовательностей $(a_0, \dots, a_n, \dots)$ с коэффициентами из K, в которых лишь конечное число ненулевых коэффициентов.

2) *Сложение* многочленов покоэффициентное:

$(a_0, \dots, a_n, \dots) + (b_0, \dots, b_n, \dots) := (a_0 + b_0, \dots, a_n + b_n, \dots)$.

3) Определим *умножение* многочленов:

$(a_0, \dots, a_n, \dots) \cdot (b_0, \dots, b_n, \dots) = (c_0, \dots, c_n, \dots)$, где

$c_n = \sum\limits_{i=0}^{n} a_i b_{n-i}$.

$a_0 * b_n + a_1 * b_{n-1} + a_2 * b_{n-2} + \dots + a_n * b_0 = c_n$

Пример:

(a_0, a_1, a_2, a_3) и (b_0, b_1, b_2) => (c_0, c_1, c_2, c_3)

$c_0 = a0 * b0$

$c1 = a_0 * b_1 + a_1 * b_0$

$c2 = a_0 * b_2 + a_1 * b_1 + a_2 * b_0$

$c3 = a_0 * b_3 + a_1 * b_2 + a_2 * b_1 + a_3 * b_0$

4) *Степень* многочлена $f = (a_0, \dots, a_n, \dots)$ — это максимальный номер ненулевого коэффициента (обозначение: $\deg(f)$). Отдельно определим степень многочлена $0 := (0, \dots, 0, \dots)$: положим $\deg(0) := -\infty$. Если $\deg(f) = n \in \mathbb{N}_0$, то a_n называется *старшим коэффициентом* f.

• Если $f = (a_0, \dots, a_n, \dots)$ и $\deg(f) \le n$, часто применяется запись $f(t) = a_n t^n + \dots + a_1 t + a_0$, где t — *формальная переменная*. Кольцо многочленов над кольцом K обозначается через $K[t]$, где t — переменная.

• Пусть K — коммутативное кольцо, $f, g \in K[t]$.

Свойство 1

$\deg(fg) \le \deg(f) + \deg(g)$. *Если K — кольцо без делителей 0, то* $\deg(fg) = \deg(f) + \deg(g)$.

Доказательство. • Если один из многочленов f и g равен 0, то несложно проверить, что произведение также равно 0. Тогда $\deg(fg) = -\infty = \deg(f) + \deg(g)$ (так как $-\infty$ при сложении с любой возможной степенью даст $-\infty$.

• Пусть $\deg(f) = n$, $\deg(g) = m$, где $m, n \in \mathbb{N}_0$, $f = (a_1, \dots, a_s, \dots)$, $g = (b_1, \dots, b_s, \dots)$ и $fg = (c_1, \dots, c_s, \dots)$.

• При $k > n + m$ имеем $c_k = (\sum\limits_{i=0}^{n-1} a_i b_{k-i}) + (\sum\limits_{i=n}^{k} a_i b_{k-i}) = 0$.

(В первой сумме $k - i > m$, поэтому $b_{k-i} = 0$. Во второй сумме $i > n$, поэтому $a_i = 0$.)

• Значит, $\deg(fg) \le \deg(f) + \deg(g)$.

(k> n+m: k – n > m и при i от 0 до n-1 k – i > m => $b_{k-i} = 0$)
(при i от n до k i > n => $a_i = 0$)

• $c_{n+m} = (\sum\limits_{i=0}^{n-1} a_i b_{n+m-i}) + a_n b_m + (\sum\limits_{i=n+1}^{n+m} a_i b_{n+m-i}) = a_n b_m \ne 0$, если K — без делителей 0. В этом случае $\deg(fg) = m + n$.

• (В первой сумме $n + m - i > m$, поэтому $b_{n+m-i} = 0$. Во второй сумме $i > n$, поэтому $a_i = 0$.) □

Алгебра. Глава
3. Многочлены.
Д. В. Карпов

Свойство 2

$\deg(f + g) \le \max(\deg(f), \deg(g))$. *Если* $\deg(f) \ne \deg(g)$, *то* $\deg(f + g) = \max(\deg(f), \deg(g))$.

Доказательство. • $f = (a_1, \dots, a_n, \dots)$, $g = (b_1, \dots, b_n, \dots)$.

• При $k > \max(\deg(f), \deg(g))$ имеем $a_k = b_k = 0$, а значит и $a_k + b_k = 0$. Следовательно, $\deg(f + g) \le \max(\deg(f), \deg(g))$.

• Пусть НУО $\deg(f) = n > \deg(g)$. Тогда $a_n + b_n = a_n + 0 \ne 0$, а значит, в этом случае $\deg(f + g) = n$. □

Пример:
$(x^3 + x^2 + x) + (-x^3 + x^2 + x) = 2x^2 + 2x$
$(x^3 + x^2 + x) + (x^2 + 1) = (x^3 + 2x^2 + x + 1)$

Теорема 1

Пусть K — коммутативное кольцо. Тогда $K[t]$ — тоже коммутативное кольцо. Если при этом K — кольцо с 1, то $K[t]$ — тоже с 1.

Доказательство. Ассоциативность и коммутативность сложения в $K[t]$ следуют из ассоциативности и коммутативности сложения в K (так как сложение покоэффициентное).

Ноль. Несложно проверить, что многочлен 0 будет нолем в $K[t]$.

Обратный элемент по сложению. Для $f = (a_0, \dots, a_n, \dots)$ положим $-f := (-a_0, \dots, -a_n, \dots)$.

Коммутативность умножения. Пусть $f = (a_0, \dots, a_n, \dots,)$ и $g = (b_0, \dots, b_n, \dots,)$, $fg = (d_0, \dots, d_n, \dots)$ и $gf = (d'_0, \dots, d'_n, \dots)$. Тогда $d_n = \sum\limits_{i=0}^{n} a_i b_{n-i} = \sum\limits_{j=0}^{n} b_j a_{n-j} = d'_n$.

Дистрибутивность. Пусть $h = (c_0, \dots, c_n, \dots,)$, $(f+g)h = (d_o, \dots, d_n, \dots,)$, $fh = (p_0, \dots, p_n, \dots,)$ и $gh = (q_0, \dots, q_n, \dots,)$. Тогда $d_n = \sum\limits_{i=0}^{n}(a_i + b_i)c_{n-i} = (\sum\limits_{i=0}^{n} a_i c_{n-i}) + (\sum\limits_{i=0}^{n} b_i c_{n-i}) = p_n + q_n$, а это коэффициент многочлена $fh + gh$.

Ассоциативность умножения. Пусть $fg = (d_0, \dots, d_n, \dots)$ и $(fg)h = (p_0, \dots, p_n, \dots)$. Тогда

$$p_n = \sum_{k=0}^{n} d_k c_{n-k} = \sum_{k=0}^{n}(\sum_{i=0}^{k} a_i b_{k-i})c_{n-k} = \sum_{i,j,\ell\in\mathbb{N}_0,\ i+j+\ell=n} a_i b_j c_\ell.$$

При другом порядке скобок, очевидно, получится то же самое.

Единица. Если существует $1 \in K$, то несложно проверить, что $1 := (1, 0, \dots, 0, \dots)$ — единица в $K[t]$. □

Билет 4: *Теорема о делении с остатком в кольце многочленов над полем*

Теорема о делении с остатком в кольце многочленов над полем.

Теорема 2

Пусть K — поле, $f, g \in K[t]$, причем $g \neq 0$. Тогда существуют единственные такие $q, r \in K[t]$, что $f = gq + r$ и $\deg(r) < \deg(g)$.

• Многочлен r из этого представления называется остатком от деления f на g.

Доказательство. Пусть $\deg(f) = n$, $\deg(g) = m$, $f(t) = a_n t^n + \dots + a_0$ и $g(t) = b_m t^m + \dots + b_0$.

$\exists$. • Индукция по $\deg(f)$. База для случая $n < m$: тогда подходит $q = 0$ и $r = f$.

Переход. • Пусть $n \geq m$ и для многочленов степени менее n утверждение доказано.

• Так как $f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} \cdot g(t)$ имеет степень $\deg(f_1) < n$, по индукционному предположению, $f_1 = q_1 g + r$, где $\deg(r) < m$.

• Тогда $f(t) = (q_1(t) + \frac{a_n}{b_m} t^{n-m}) \cdot g(t) + r(t)$ — искомое представление для f.

Алгебра. Глава 3. Многочлены.
Д. В. Карпов

! Пусть $f = q_1 g + r_1 = q_2 g + r_2$, где $\deg(r_1) < m$ и $\deg(r_2) < m$. Тогда $r_1 - r_2 = g(q_2 - q_1)$.

• Пусть $q_1 \neq q_2$. Тогда $\deg(q_2 - q_1) \in \mathbb{N}_0$ и $\deg((q_2 - q_1)g) = \deg(q_2 - q_1) + \deg(g) \geq m$. С другой стороны, $\deg(r_1 - r_2) \leq \max(\deg(r_1), \deg(r_2)) < m$, противоречие.

• Значит, $q_1 = q_2$, тогда и $r_1 = r_2$. □

Билет 5: *Делимость многочленов. Свойства.*

Делимость многочленов

Определение

Пусть K — поле, $f, g \in K[t]$, $g \neq 0$. Говорят, что f **делится** на g (обозначение $f \vdots g$), если существует такой $h \in K[t]$, что $f = gh$.

Свойство 1

Если $f \vdots g$ и $g \vdots h$, то $f \vdots h$.

Доказательство. Тогда $f = pg$ и $g = qh$, где $p, q \in K[t]$, откуда следует $f = (pq)h$. □

Свойство 2

Пусть $f, g \vdots h$, а $p, q \in K[t]$. Тогда $fp + gq \vdots h$.

Доказательство. Тогда $f = ah$ и $g = bh$, где $a, b \in K[t]$, откуда следует $fp + gq = (ap + bq)h$. □

Свойство 3

Пусть $f, g \in K[t]$, $f \neq 0$, $f \vdots g$. Тогда $\deg(f) \geq \deg(g)$.

Доказательство. Тогда $f = gh$, где $h \in K[t]$, причем понятно, что $h \neq 0$. Следовательно, $\deg(f) = \deg(g) + \deg(h) \geq \deg(g)$. □

Свойство 4

Пусть $f, g \in K[t]$, $f, g \neq 0$, $f \vdots g$ и $\deg(f) = \deg(g)$. Тогда $f \sim g$.

Доказательство. • Тогда $f = gh$, где $h \in K[t]$, и $\deg(g) = \deg(f) = \deg(g) + \deg(h)$.

• Следовательно, $\deg(h) = 0$, значит, $h \in K$, $h \neq 0$, то есть, $f \sim g$. □

Свойство 5

Пусть $f, g \in K[t]$, $f, g \neq 0$, $f \vdots g$ и $g \vdots f$. Тогда $f \sim g$.

Доказательство. Тогда $\deg(f) \geq \deg(g)$ и $\deg(g) \geq \deg(f)$. Следовательно, $\deg(f) = \deg(g)$. По Свойству 4, $f \sim g$. □

Идеалы в кольце многочленов над полем.

Теорема 3

Пусть K — поле, а I — Идеал в $K[t]$. Тогда $I = dK[t]$ для некоторого $d \in K[t]$.

Доказательство. • Если $I = \{0\}$, то подойдет $d = 0$.

• Пусть $I \neq \{0\}$. Тогда рассмотрим все ненулевые многочлены из I и найдем из них многочлен наименьшей степени d.

• Докажем, что все многочлены из I делятся на d (тогда $I = dK[t]$).

• Пусть $f \not\vdots\, d$, тогда поделим f на d с остатком: $f = qd + r$, $\deg(r) < \deg(d)$, $r \neq 0$.

• Так как $f, d \in I$, мы имеем $r = f - dq \in I$. Противоречие с минимальностью $\deg(d)$. $\square$